Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A method of secure information distribution between nodes, the method comprising:

performing, by a first node, a handshake process with an adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group;

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group; and

distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

Claim 2 (Original): The method of claim 1, further comprising:

prior to providing the secure information to the adjacent node, performing the handshake process with another adjacent node.

Claim 3 (Original): The method of claim 1, further comprising:

establishing an encryption key with the adjacent node.

Claim 4 (Original): The method of claim 3, wherein the encryption key comprises a public key.

Claim 5 (Original): The method of claim 3, wherein the encryption key comprises a symmetric key.

Claim 6 (Original): The method of claim 3, wherein the secure information is distributed along with an encryption key.

Claim 7 (Original): The method of claim 1, wherein the action of performing the handshaking process comprises:

using a one way function f(x) to determine if the adjacent node is a member of the secure group.

Claim 8 (Original): The method of claim 7, wherein the one way function f(x) is a secure hash function.

Claim 9 (currently amended): The method of claim 1, wherein the action of performing the handshaking process comprises:

providing, by a first node, a component value A1 for a one way function f(x);

providing, by the adjacent node, a component value B1 as a challenge to the first node; and

applying the component values A1 and B1, and ~~a~~ the key value ~~SGK~~ to the one way function f(x) to generate a value y.

Claim 10 (Original): The method of claim 9, wherein the one way function f(x) is a secure hash function.

Claim 11 (Original): The method of claim 1, wherein the secure information comprises a password.

Claim 12 (Original): The method of claim 1, wherein the secure information comprises a key for secure communication.

Claim 13 (Original): The method of claim 1, further comprising:

distributing secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

Claim 14 (Original): The method of claim 1, wherein the action of performing the handshake process comprises:

performing the handshake process with the adjacent node once for every fixed time amount T.

Claim 15 (Original): The method of claim 1, further comprising:

after detecting the presence of another node that is not in an adjacency set, attempting to handshake with that another node if a detecting node and the another node both have a handshake time remaining value of zero (0).

Claim 16 (Original): The method of claim 1, further comprising:

determining an age of the secure information so that each node in the secure group will store a latest version of the secure information.

Claim 17 (Original): The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a sequence number of the secure information to determine the age of the secure information.

Claim 18 (Original): The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking a date of modification of the secure information to determine the age of the secure information.

Claim 19 (Original): The method of claim 16, wherein the action of determining the age of the secure information comprises:

checking an elapsed time since a previous modification of the secure information to determine the age of the secure information.

Claim 20 (Original): The method of claim 1, further comprising:

resolving an ambiguity between a received updated secure information and currently stored secure information

by selecting the secure information with a larger data value.

Claim 21 (currently amended): The method of claim 1, further comprising:

increasing a security of the secure group by widening ~~a secure group~~ the key ~~(SGK)~~ value which is known by each node in the secure group.

Claim 22 (Original): The method of claim 1, further comprising:

decreasing an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

Claim 23 (Original): The method of claim 1, further comprising:

allowing for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of handshakes and TB is a time amount between burst of handshakes.

Claim 24 (Original): The method of claim 1, further comprising:

preventing a single node in the secure group from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW $\pm$ TR between handshake attempts, where TW is a fixed configurable time

amount and TR is a random amount of time that is bounded by a user-specified bound range.

Claim 25 (currently amended): An apparatus for secure information distribution between nodes, the apparatus comprising:

a node configured to performing a handshake process with an adjacent node to determine membership in a secure group, and distribute secure information to the adjacent node, if the adjacent node is proven to be a member of the secure group;

wherein the handshake process comprises requiring each of the node and the adjacent node to prove a key value that is associated with the secure group; and

wherein each of the node and the adjacent node has an identifier value that is associated with the secure group in order for the node and the adjacent node to have membership in the secure group.

Claim 26 (Original): The apparatus of claim 25, wherein the node performs the handshake process with another adjacent node, prior to providing the secure information to the adjacent node.

Claim 27 (Original): The apparatus of claim 25, wherein the node is configured to establish an encryption key with the adjacent node.

Claim 28 (Original): The apparatus of claim 25, wherein the encryption key comprises a public key.

Claim 29 (Original): The apparatus of claim 25, wherein the encryption key comprises a symmetric key.

Claim 30 (Original): The apparatus of claim 27, wherein the secure information is distributed along with an encryption key.

Claim 31 (Original): The apparatus of claim 25, wherein the node is configured to use a one way function f(x) to determine if the adjacent node is a member of the secure group.

Claim 32 (Original): The apparatus of claim 31, wherein the one way function f(x) is a secure hash function.

Claim 33 (currently amended): The apparatus of claim 25, wherein the node is configured to provide a component value A1 for a one way function f(x), and wherein the adjacent node is configured to provide a component value B1 as a challenge to the first node; and wherein the node and adjacent node are configured to apply the component values A1 and B1, and ~~a~~ the key value ~~SGK~~ to the one way function f(x) to generate a value y.

Claim 34 (Original): The apparatus of claim 33, wherein the one way function f(x) is a secure hash function.

Claim 35 (Original): The apparatus of claim 25, wherein the secure information comprises a password.

Claim 36 (Original): The apparatus of claim 25, wherein the secure information comprises a key for secure communication.

Claim 37 (Original): The apparatus of claim 25, wherein the node is configured to distribute the secure information to each adjacent node that is a member of the secure group, in response to an update of the secure information.

Claim 38 (Original): The apparatus of claim 25, wherein the node is configured to perform the handshake process with the adjacent node once for every fixed time amount T.

Claim 39 (Original): The apparatus of claim 25, wherein the node is configured to attempt to handshake with another node if the node and the another node both have a handshake time remaining value of zero (0).

Claim 40 (Original): The apparatus of claim 25, wherein the node is configured to determine an age of the secure information so that each node in the secure group will store a latest version of the secure information.

Claim 41 (Original): The apparatus of claim 25, wherein the node is configured to check a sequence number of the secure information to determine the age of the secure information.

Claim 42 (Original): The apparatus of claim 25, wherein the node is configured to check a date of modification of the secure information to determine the age of the secure information.

Claim 43 (Original): The apparatus of claim 25, wherein the node is configured to check an elapsed time since a previous modification of the secure information to determine the age of the secure information.

Claim 44 (Original): The apparatus of claim 25, wherein the node is configured to resolve an ambiguity between a received updated secure information and currently stored secure information by selecting the secure information with a larger data value.

Claim 45 (currently amended): The apparatus of claim 25, wherein the node is configured to increase a security of the secure group by widening ~~a secure group~~ the key ~~(SGK)~~ value which is known by each node in the secure group.

Claim 46 (Original): The apparatus of claim 25, wherein the node is configured to decrease an amount of time between symmetric key regeneration (TK) to increase the security of the secure group.

Claim 47 (Original): The apparatus of claim 25, wherein the node is configured to allow for rapid construction of the secure group by transmitting a burst of NB handshakes for every amount of time TB, where NB is the number of

handshakes and TB is a time amount between burst of handshakes.

Claim 48 (Original): The apparatus of claim 25, wherein the node is prevented from attempting to handshake with numerous nodes to avoid excessive joins, by establish membership with one adjacent node at a time, and waiting at time TW ± TR between handshake attempts, where TW is a fixed configurable time amount and TR is a random amount of time that is bounded by a user-specified bound range.

Claim 49 (currently amended): An apparatus for secure information distribution between nodes, the apparatus comprising:

means for performing a handshake process ~~with~~ between a first node and an adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group;

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group; and

means for distributing secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

Claim 50 (currently amended): An article of manufacture, comprising:

a machine-readable medium having stored thereon instructions to:

perform a handshake process ~~with~~ between a first node and an adjacent node to determine membership in a secure group;

wherein the handshake process comprises requiring each of the first node and the adjacent node to prove a key value that is associated with the secure group;

wherein each of the first node and the adjacent node has an identifier value that is associated with the secure group in order for the first node and the adjacent node to have membership in the secure group; and

distribute secure information from the first node to the adjacent node, if the adjacent node is proven to be a member of the secure group.

Claim 51 (new): The method of claim 1, wherein the handshake process further comprises:

applying a one way function to the key value so that the one way function generates a calculated value y, and transmitting the calculated value y between the first node and the adjacent node.

Claim 52 (new): The method of claim 1,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

Claim 53 (new): The apparatus of claim 25, wherein the handshake process further comprises:

applying a one way function to the key value so that the one way function generates a calculated value y, and transmitting the calculated value y between the node and the adjacent node.

Claim 54 (new): The apparatus of claim 25,

wherein the node belongs to the secure group if the node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

Claim 55 (new): The apparatus of claim 49, wherein the handshake process further comprises:

applying a one way function to the key value so that the one way function generates a calculated value y, and transmitting the calculated value y between the first node and the adjacent node.

Claim 56 (new): The apparatus of claim 49,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.

Claim 57 (new): The article of manufacture of claim 50, wherein the handshake process further comprises:

applying a one way function to the key value so that the one way function generates a calculated value y, and transmitting the calculated value y between the first node and the adjacent node.

Claim 58 (new): The article of manufacture of claim 50,

wherein the first node belongs to the secure group if the first node contains the identifier value and proves the key value during the handshake process,

wherein the adjacent node belongs to the secure group if the adjacent node contains the identifier value and proves the key value during the handshake process, and

wherein the secure information is distributed only between nodes in the secure group.